REMARKS/ARGUMENTS

Claims 1-32 are pending in the present application. Claims 1-32 have been rejected. The Abstract has been amended to shorten the Abstract. Substitute drawings for Figures 5 and 6 are filed herewith to respond to the objections by the draftsperson.

Applicants respectfully respond to this Office Action.

A. Claims 1-32 Rejected under 35 U.S.C. § 102

The Examiner rejected claims 1-32 under 35 U.S.C. § 102(a) as being anticipated by Drake, U.S. Patent No. 6,006,328 (hereinafter, "Drake"). This rejection is respectfully traversed.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131 (July 1998) (citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). "The identical invention must be shown in as complete detail as is contained in the . . . claim." M.P.E.P. § 2131 (July 1998) (citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)). In addition, "the reference must be enabling and describe the applicant's claimed invention sufficiently to have placed it in possession of a person of ordinary skill in the field of the invention." In re Paulsen, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994).

Claim 1 recites "accessing instructions that access observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program." Drake does not disclose this claim element. The Examiner has cited the following portion of Drake as disclosing this claim element:

> This invention seeks to provide computer software having enhanced security features, to a process which substantially enhances the security of computer software (hereafter referred to as the improved process) and to a method by which to apply said improved process (hereafter referred to as the applicator).
>
> The improved process consists of including computer code to automatically detect tampering of said computer software, and computer code to prevent the theft of ID-Data by replacing existing vulnerable (to rogue software eavesdropping or attack) software or operating system code with secure equivalents which utilise anti-spy techniques (as described later in this document).

> Preferably, the improved process also consists of including computer code to prevent decompilation, reverse-engineering, and disassembly by the inclusion of obfuscating code inserts, and the use of executable encryption.
>
> Preferably, the improved process also consists of including code to prevent execution-tracing and debugging by the use of code designed to detect and prevent these operations.
>
> Preferably, the improved process consists of, or also includes, human-recognisable audio-visual components which permit the authenticity of said computer software to be easily verified by the user on each invocation using techniques described later in this document.
>
> The idea which lead to the creation of this invention can be summarised as follows: If a piece of computer software that is executing can be shown to be the genuine article, and this software can protect itself against eavesdropping, and this software can prevent tampering of itself, then is it possible for this software to function in a secure manner, even within an insecure operating system. This invention permits the creation of such a piece of computer software--having a tangible, useful security advantage and hence improving its value.

Drake, Col. 3, lines 32-67.

This portion of Drake does not disclose "accessing instructions that access observer data, the observer data including data descriptive of an observer program." It does mention "rogue software eavesdropping" (Col. 3, lines 41-42) and "anti-spy techniques" (Col. 3, lines 43), but these generic terms do not disclose this claim element. Claim 1 specifically requires "accessing instructions that access observer data," wherein "the observer data include[es] data descriptive of an observer program." Furthermore, "the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program."

Claim 1 also recites "comparing instructions that compare the observer data with memory data read in from memory to determine whether the observer program is present on the computer system." Drake does not disclose this claim element. The Examiner has cited the following portion of Drake as disclosing this claim element:

Aspect 3. Detecting Tampering

> As hereinbefore described, it is desirable to detect tampering, since this may lead to the reduction of software security.
>
> ***This can be achieved with the use of code which is protected from disassembly and examination through obfuscation and encryption, which re-***

> ***reads its own external-image and compares it with its known memory image or precalculated check-data to detect hot-patching (ie. the modification of software sometime after it has been loaded from disk, but (usually) before execution of the modified section has commenced).***
>
> ***Additionally, the software can scan the memory image of itself one or more times, or continuously, to ensure that unexpected alterations do not occur.***
>
> Certain modifications to the external copy of software are reflected in subtle changes to the environment in which the modified software will be executed (for example: the size of the code, if altered, will be reflected in the initial code size value supplied to the executing program being incorrect.). Additionally, certain modification to the operating system and environment of said software can also be monitored (for example: certain interrupt vector table pointers in Intel-processor applications) to detect unexpected changes by rogue software. These changes can also be detected to prevent tampering.
>
> Once tampering is detected, program flow-of-control needs to be changed so that the potential compromise associated with ID-Data theft is avoided. This may be the security-enhanced program terminating with a message indicating that its integrity has been compromised before all of the ID Data is entered. Alternatively, the fact that tampering has been detected may be kept secret and the ID-Data retrieved, however, immediately upon retrieval, the ID-Data entered can be invalidated thus preventing access to that which the now potentially compromised ID-Data would have otherwise allowed. This latter method allows for the possibility of security-enhanced software informing remote or other authorities that tampering was detected and possibly other information, such as what specifically was altered and by whom. Care must be taken to ensure the integrity of the "remote-informing" code before ID-Data entry is permitted.

Drake, Col. 6, lines 5-48 (emphasis added).

This portion of Drake does not disclose “comparing instructions that compare the observer data with memory data read in from memory to determine whether the observer program is present on the computer system.” This section of Drake discloses aspects of detecting tampering, as the heading in Drake indicates. Recall that claim 1 recited above “the observer data including data descriptive of an observer program, the observer program being programmed to observe a user’s activities on the computer system and also operating to create data from the observing of the observer program.”

Claim 1 further recites “outputting instructions that obtain the results and provide the results for a user.” Claim 1 also states “wherein the results generated indicate whether the observer program is present on the computer system.” Drake does not disclose this claim limitation. The Examiner has cited Col. 6, lines 5-48 (quoted above) and the following portion of Drake as disclosing this claim element:

> Detailed hereafter are several security-enhancing techniques to combat eavesdropping. Security is provided by (a) hampering examination of software-code operating system code or or parts thereof through the use of the encryption or partial encryption of said code, (b) preventing the disassembly of said code through the inclusion of dummy instructions and prefixes and additional code to mislead and hamper disassembly (ie: obfuscating inserts), (c) preventing the computerised tracing of the execution of said code (for example: with code debugging tools) through the use of instructions to detect, mislead, and hamper tracing, (d) preventing tampering of said code through the use of scanning to locate alterations, either or both on-disk and in memory either once at the start of execution, or continuously upon certain events, or (e) preventing ID-Data theft through the inclusion of secure input/output routines (for example: routines to bypass the standard operating system keyboard calls and use custom-written higher-security routines as a replacement) to replace insecure computer-system routines. Hereafter, the term anti-spy will be used to refer to any combination of one or more of the abovementioned techniques [(a) through (e) or parts thereof] used to prevent eavesdropping.

Drake, Col. 4, lines 47-65.

These portions of Drake cited by the Examiner do not disclose "outputting instructions that obtain the results and provide the results for a user." Recall that claim 1 also states "wherein the results generated indicate whether the observer program is present on the computer system." The portion of in Col. 6 cited by the Examiner is discussing tampering and states "[o]nce tampering is detected, program flow-of-control needs to be changed so that the potential compromise associated with ID-Data theft is avoided. This may be the security-enhanced program terminating with a message indicating that its integrity has been compromised before all of the ID Data is entered." Thus, this section discloses that when tampering has been detected, a message indicating that the program's integrity has been compromised. However, this is not the same as the claim element at issue.

As set forth above, Drake does not disclose every element of claim 1. Claims 2-15 depend directly or indirectly from claim 1. Thus, Applicant respectfully requests that the rejection of claims 2-15 be withdrawn for at least the same reasons.

Claim 16 recites "means for accessing observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program." Drake does not disclose this claim element. The Examiner has cited Col. 3, lines 32-67 (quoted above) of Drake as disclosing this claim element. This portion of Drake does not disclose "means for accessing observer data, the observer data including data descriptive of an observer program." It does mention "rogue software eavesdropping" (Col. 3, lines 41-42) and "anti-spy techniques" (Col. 3, lines 43), but these generic terms do not disclose this claim element.

Claim 1 also recites "means for comparing the observer data with memory data to determine whether the observer program is present on the computer system." Drake does not disclose this claim element. The Examiner has cited Col. 6, lines 5-48 of Drake (quoted above) as disclosing this claim element. This portion of Drake does not disclose "means for comparing the observer data with memory data to determine whether the observer program is present on the computer system." This section of Drake discloses aspects of detecting tampering, as the heading in Drake indicates. Recall that claim 1 recited above "the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program."

Claim 16 further recites "means for outputting the results for a user." Claim 16 also states "wherein the results generated indicate whether the observer program is present on the computer system." Drake does not disclose this claim limitation. The Examiner has cited Col. 6, lines 5-48 (quoted above) and Col. 4, lines 47-65 (quoted above) as disclosing this claim element. These portions of Drake cited by the Examiner do not disclose "means for outputting the results for a user." Recall that claim 1 also states "wherein the results generated indicate whether the observer program is present on the computer system." The portion of in Col. 6 cited by the Examiner is discussing tampering and states "[o]nce tampering is detected, program flow-of-control needs to be changed so that the potential compromise associated with ID-Data theft is avoided. This may be the security-enhanced program terminating with a message indicating that its integrity has been compromised before all of the ID Data is entered." Thus, this section discloses that when tampering has been detected, a message indicating that the program's integrity has been compromised. However, this is not the same as the claim element at issue.

Claim 17 recites "accessing observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program." Drake does not disclose this claim element. The Examiner has cited Col. 3, lines 32-67 (quoted above) of Drake as disclosing this claim element. This portion of Drake does not disclose "accessing observer data, the observer data including data descriptive of an observer program." It does mention "rogue software eavesdropping" (Col. 3, lines 41-42) and "anti-spy techniques" (Col. 3, lines 43), but these generic terms do not disclose this claim element.

Claim 17 also recites "comparing the observer data with memory data read in from memory to determine whether the observer program is present on the computer system." Drake does not disclose this claim element. The Examiner has cited Col. 6, lines 5-48 (quoted above) of Drake as disclosing this claim element. This portion of Drake does not disclose "comparing the observer data with memory data read in from memory to determine whether the observer program is present on the computer system." This section of Drake discloses aspects of detecting tampering, as the heading in Drake indicates. Recall that claim 17 recited above "the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program."

Claim 17 further recites "outputting the results for a user." Claim 17 also states "wherein the results generated indicate whether the observer program is present on the computer system." Drake does not disclose this claim limitation. The Examiner has cited Col. 6, lines 5-48 (quoted above) and Col. 4, lines 47-65 (quoted above) of Drake as disclosing this claim element. These portions of Drake cited by the Examiner do not disclose "outputting the results for a user." Recall that claim 17 also states "wherein the results generated indicate whether the observer program is present on the computer system." The portion of in Col. 6 cited by the Examiner is discussing tampering and states "[o]nce tampering is detected, program flow-of-control needs to be changed so that the potential compromise associated with ID-Data theft is avoided. This may be the security-enhanced program terminating with a message indicating that its integrity has been compromised before all of the ID Data is entered." Thus, this section discloses that when tampering has been detected, a message indicating that the program's integrity has been compromised. However, this is not the same as the claim element at issue.

As set forth above, Drake does not disclose every element of claim 17. Claims 18 and 19 include similar limitations as claim 17. Thus, Applicant respectfully requests that the rejections of claims 18 and 19 be withdrawn for at least the same reasons.

Claim 20 recites "accessing instructions that access observer data, the observer data including data descriptive of an observer program, the observer program being programmed to observe a user's activities on the computer system and also operating to create data from the observing of the observer program." Drake does not disclose this claim element. The Examiner has cited Col. 3, lines 32-67 of Drake as disclosing this claim element. This portion of Drake does not disclose "accessing instructions that access observer data, the observer data including data descriptive of an observer program." It does mention "rogue software eavesdropping" (Col. 3, lines 41-42) and "anti-spy techniques" (Col. 3, lines 43), but these generic terms do not disclose this claim element.

Claim 20 also recites "altering instructions that alter a file relating to the observer program such that the operation of the observer program is changed." Drake does not disclose this claim element. The Examiner has cited the following portion of Drake as disclosing this claim element:

> Obfuscating inserts can successfully prevent automatic disassembly. Obfuscation is achieved by following unconditional jump instructions (for example, Intel JMP or CLC/JNC combination or CALL (without a return expected) or any flow-of-control altering instruction (which is known not to return to the usual place) with one or more dummy op-code bytes which will cause subsequent op-codes to be erroneously disassembled (for example, the Intel 0xEA prefix will cause disassembly of the subsequent 4 op-codes to be incorrect, displaying them as the offset to the JMP instruction indicated by the 0xEA prefix instead of the instructions they actually represent).
>
> Dummy instructions may also be included to hamper disassembly by deliberately

> misleading a disassembler into believing a particular flow of control will occur, when in fact it will not.
>
> Flow of control can be designed to occur based upon CPU flag values determined from instructions executed a long time ago. Together with tracing preventing, this makes manual disassembly nearly impossible.

Drake, Col. 5, lines 42-62.

These portions of Drake do not disclose "altering instructions that alter a file relating to the observer program such that the operation of the observer program is changed." These portions of Drake are under the section entitled "Aspect 2. Preventing Disassembly and Examination." Drake, Col. 5, line 36. To help put this section of Drake into context it is helpful to read the paragraph immediately preceding lines 42-62 which reads "[a]s hereinbefore described, it is desirable to hamper disassembly (or de-compilation or reverse engineering) to protect software against eavesdropping and tampering, and to hinder examination of said software which might lead to secret security problems or mistakes being disclosed." Drake, Col. 5, lines 37-41. Thus, Col. 5, lines 42-62 of Drake disclose what to put into a program to prevent disassembly and examination. This is not disclosing any "altering instructions that alter a file relating to the observer program such that the operation of the observer program is changed."

The Examiner has also cited this portion of Drake as disclosing "altering instructions that alter a file relating to the observer program such that the operation of the observer program is changed:"

> Bypassing system routines (eg: in DOS, using direct memory writes instead of DOS system calls to revector interrupts) will further hamper debugging and rogue software monitoring, as will unravelling loop constructs (which will make tracing long and cumbersome). Code checksums and operating-system checks (eg: interrupt table pointers) can be designed to detect debug-breakpoint instruction inserts or other modifications. Using the result of the checksum for some obscure purpose (eg: decryption, or (much later) control-flow changes) will further hamper tracing.

Drake, Col. 8, lines 3-12.

These portions of Drake does not disclose "altering instructions that alter a file relating to the observer program such that the operation of the observer program is changed." Rather, this discloses how to "hamper debugging and rogue software monitoring" and how to "detect debug-breakpoint instruction inserts or other modifications."

As set forth above, Drake does not disclose every element of claim 20. Claims 21-28 depend directly or indirectly from claim 20. Thus, Applicant respectfully requests that the rejection of claims 21-28 be withdrawn for at least the same reasons. Claims 29-32 also include similar limitations as described in relation to Claim 20. Thus, Applicants respectfully request that the rejection of claims 29-32 be withdrawn for at least the same reasons.

Applicant respectfully asserts that claims 1-32 are patentably distinct from the cited references, and requests that a timely Notice of Allowance be issued in this case. If there are any remaining issues preventing allowance of the pending claims that may be clarified by telephone, the Examiner is requested to call the undersigned.

Respectfully submitted,

Wesley L. Austin
Reg. No. 42,273
Attorney for Applicant(s)

Date: May 11, 2004

Wesley L. Austin, Esq.
Trapware Corporation
1987 S. Bluebell Dr.
Bountiful, UT 84010
Telephone: (801) 296-0597